Expertise
and insight
for the future

Tesfaye Wubu

Migration of Traditional IT System to Cloud Computing with Amazon Web Services

Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Program in Information Technology

Bachelor's Thesis

18 April 2020

Author	Tesfaye Wubu
Title	Migration of Traditional IT System to Cloud Computing with Amazon Web Services
Number of Pages	41 pages
Date	January 18,2020
Degree	Bachelor of Engineering
Degree Program	Information Technology
Professional Major	Cloud Computing and IoT
Instructors	Erik Pätynen, Senior Lecturer

The purpose of this project was to migrate the on-premises information technology systems of an organization to the cloud. The migration was implemented using the Amazon Web Services technology.

The transformation process to the cloud involved studying the existing system of the organization, designing 3-tier cloud architecture on the web, application and database tiers. The implementation was done using the tools and technologies of the Amazon Web Services.

The migration of the existing traditional system resulted in delivering better storage, computing, databases and other services. Moreover, the work resulted in improved reliability and performance by minimizing the cost of administration and support. The Amazon Web Services provided cutting edge technologies and tools to migrate to the cloud.

Keywords	Cloud Computing, Amazon Web Services, EC2, ELB, Auto Scaling

Contents

1 Introduction

The focus of this thesis is migration of traditional information systems to the cloud using the Amazon Web Service (AWS) technology. A case study was carried out on institutions of financial services, specifically on a bank.

The existing IT system of the financial institution was traditional, and it hosted infrastructure locally. Branch offices were not connected efficiently to access and share resources with customers, the head office and other stakeholders. In the project, Amazon Web Services technologies were implemented to migrate the existing traditional IT infrastructure to the cloud. The transformation benefited the organization in providing cutting edge infrastructure for data access and application management in a manner of cost effectiveness, efficiency, speed and agility. Furthermore, the adopted cloud system enabled the organization to have solutions and services of storage, databases, and networks.

This thesis covers theoretical concepts of cloud computing and Amazon Web Services technologies. It proposes a 3-tier architecture design (web tier, application tier and database tier), and based on the design a solution was implemented, providing infrastructure as a service using the Amazon web service technology. Even though Amazon Web Services cover a various range of technologies, the scope of this thesis is limited to some of the technological aspects.

2 Cloud Computing

2.1 Overview

Cloud computing could be understood in different ways among people, and the idea of cloud computing can be perplexing. Cloud computing simply means the collection of technologies, which is the understanding that comes to mind. Certainly, cloud computing is built up with a number of technologies. Different services together form the cloud. Some of the applications and tools included as services are database as a service, storage as a service, and computing as a service. [1, p. 1.] Cloud computing has turned the vision of human using computing as utility, like electricity, telephone, gas and water [2, p. 3].

Cloud computing can be defined in numerous ways. According to NIST (National Institute of Standards and Technology in the United States), cloud computing is defined as a model that delivers on demand a number of computing services of storage, software, servers, analytics and networks on the internet. [3.]

Cloud computing has become a major key player in delivery of information technology services and business models. Critical services and applications run on the cloud. The service provided by the cloud is highly available and low cost. Using cloud computing, it is possible to transform ideas to reality without any infrastructure of hardware and software procurement, installation and configuration. [4, p. 4.]

A traditional information system hosts, runs and manages all the resources locally. This type of system requires expensive financial investment for owning and running the infrastructure of hardware and software. In addition, the process of the installation and configuration of the system is time consuming.

2.2 Features of Cloud Computing

For a service to be considered as a cloud service, it is supposed to meet specific characteristics. Any web-based application cannot be a cloud application unless it meets the

characteristics of a cloud. Based on the definition of NIST there are five characteristics. [1, 3.]

On-Demand Self-services

On-demand self-services are a means of accessing resources and services independently without the involvement of an administrator. All the required procedures are automated. Such features enable access to resources fast and in a simple way. The cloud shortens the time of processing taken by on-premise IT systems. In addition, it saves cost and time for the cloud provider. [1, p. 3.]

Broad Network Access

Users require network connection to access the cloud. They can access services using different kinds of devices such as desktops, laptops, smartphones, and tablets. [4.]

Resource Pooling

Resource pooling is a characteristic of the cloud that makes it possible to share physical resources with numerous users. This feature allows the service provider to allocate free resources to other users. Virtualization is the technology applied behind the resource pooling. [1, p.5.]

Rapid Elasticity

Utilization of resources by customers raises continuously. To meet this need, the cloud should expand accordingly. The resources offered can increase, decrease or stop based on the demand. [6.]

Measured Services

Paying for the access to a cloud service is based on measured services. There are different measurement units, for instance, rate of data transfer, capacity of bandwidth, and time. [1, p. 5.]

2.3 Cloud Deployment Models

Based on the definition of NIST there are four deployment models. They are public, private, hybrid and community models. The deployment model determines where to store data and how it could be accessed. [7.]

Public Cloud

The public cloud deployment model is the popular one. In this model, the service provider controls and administers all the services on its own hardware. It is possible to share resources with other customers for cost minimization. [5.]

The public cloud has the advantage of simple and cost saving configuration, and most of the services of the cloud are managed by the provider. The user is supposed to set up extra features for accessing resources. [8.]

This model has shortcomings that may arise due to the situation that the resources are administered by an external company. Thus, the user may face limited integration and flexibility, data security issues, compliance and auditing. [1, p. 40.]

Private Cloud

In the private cloud model, the owner of the cloud is responsible for designing, administering and upgrading the infrastructure in their own private cloud. The owner of the cloud installs all the services of hardware and software needed. [7.]

The private cloud better fits for organizations that require full management on the cloud. It offers the advantage of providing improved flexibility, security and scalability for businesses, governments and commercials. [9.]

Hybrid Cloud

The hybrid cloud model has combined the advantages of both the public and the private cloud model. The private cloud can host more sensitive applications that require persistent capacity and performance, while the public cloud handles the applications that are not critical. [10.]

The hybrid cloud has the benefit of security, scalability, optimization of resources and cost saving [9]. It is characterized by more flexibility, high availability and fault tolerance. However, the implementation of the hybrid cloud is not straightforward. [1, p. 46.]

Community Cloud

The community cloud is less popular compared to private and public cloud in terms of usage. The community cloud is a better solution for a set of organizations with a common objective. [1, p. 43.]

The main benefits of the community cloud come due to sharing infrastructure that brings cost minimization. As a number of organizations share infrastructure, there is a possibility of disagreement that may happen. [1, p. 43.]

2.4 Cloud Delivery Models

According to the National Institute of Standards and Technology (NIST), there are three classifications that are based on the delivery model of the services. The services are given below / listed below. [3.]

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

Software as a Service (SaaS)

SaaS is a software solution that enables the user to access applications from service providers. The applications are accessible through a web browser. The service provider fully administers and manages the infrastructure such as servers, operating systems, networks, and applications. [11.]

There are several SaaS providers. Some of them are Microsoft Outlook, Google Drive, and Salesforce [1,55].

A SaaS implementation has specific characteristics that may vary insignificantly with respect to the provider and type of services to be provided. Some of the characteristics are customization, support and maintenance, analytics, integration and responsibilities. [1, p. 52.]

Some of the challenges that may arise on the implementation of SaaS are disparate location, multitenancy and security [1, p. 55].

Platform as a Service (PaaS)

The PaaS model enables users to acquire infrastructure for the development of applications. PaaS creates a platform for a database, development, storage, networks, servers and the operating system. [1, p. 7.]

In case of PaaS, users have full access to applications to change the application according to their requirements. However, the users have limited rights to the customization of the platform. [1, p. 64.]

PaaS benefits users in terms of cost minimization, scalability with simplicity and cost-effectiveness, and access to a variety of resources that are safe, easy and fast [13].

Infrastructure as a Service (IaaS)

IaaS is one of the cloud computing models that provides basic computing, storage and networking to users [12]. In this case, the user accesses the virtual resources without the physical presence of the hardware. In addition, the user has the right to manage and configure the computing resources. [2, p. 77.]

In the IaaS model, the hardware is stored in the datacenter of the service provider. The user can manage and configure applications and operating systems. The responsibilities of installation, management and updating of applications, the operating system, and antivirus software are part of the user activities. [1, p. 72.]

Even though IaaS enables companies to save money that would be spent on building expensive datacenters, it has some security issues. [1, p. 73.]

The cloud services delivery model can be categorized as a collection of services of a group of architecture, as shown in figure 1.

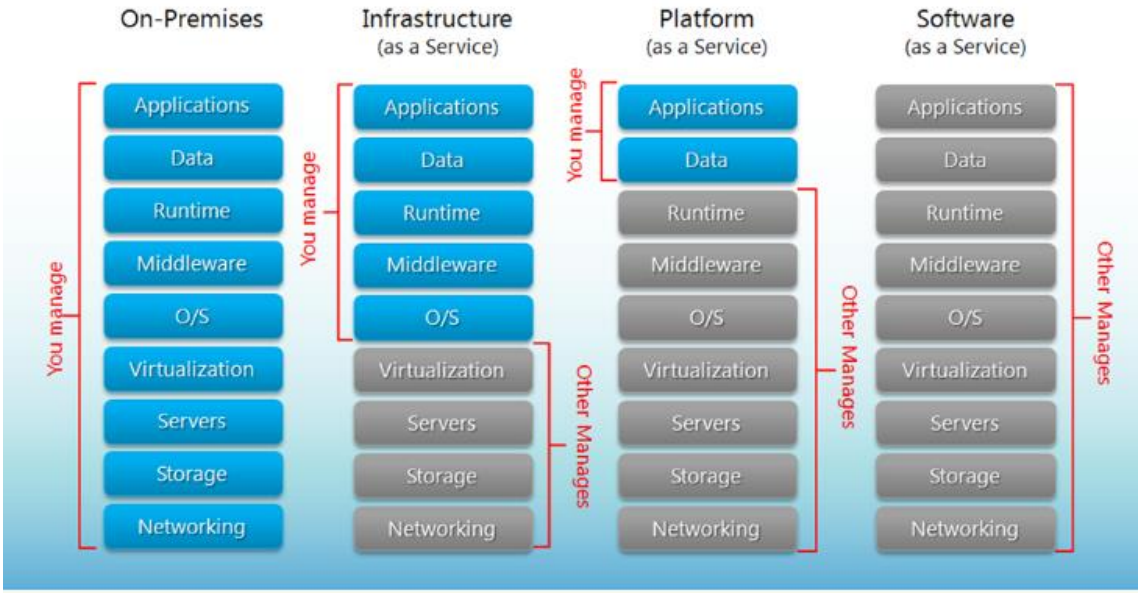


Figure 1. Separation of Responsibilities, Copied from ICT Solutions for Brilliant Minds [12].

2.5 Advantages and Disadvantages of Cloud Computing

The benefits of cloud computing are explained below.

Elastic

Resource consumption increases and drops according to workload. The elasticity features of cloud computing manage the situation by decreasing and increasing resources spontaneously. [15.]

For instance, if a company runs an application, the access load of the application varies during the day. The cloud feature puts more resources during the peak time and drops resources at other times. [15.]

Scalable

Scalability can be implemented using an initiating event such as CPU consumption, and based on this factor, the number of resources increases or drops in a few minutes [15].

Horizontal scaling (scaling out) refers putting servers that operate simultaneously to handle high workloads [15].

Vertical scaling (scaling up) is putting resources such as memory and CPU to boost the capacity of the server [15].

Cost Effective

Cloud computing charges for what has been consumed. This model is beneficial because it allows avoiding the initial cost for infrastructure and infrastructure management, paying for extra expenses and resources demanded. Moreover, it cuts down the payments for idle resources. [15.]

Secure

The cloud is more secure than traditional IT systems, preventing the infrastructure, data and applications from being attacked against. The cloud mitigates physical and digital security threats using a better method. [15.]

Global

Datacenters of cloud services providers are distributed throughout the world. Having datacenters in geographic locations that are close to the customers mitigates latency. [15.]

Reliable

Ensuring data reliability is the basic requirement of a business. Cloud service providers secure customers' data security using various techniques such as replication of data, regular and scheduled backups, and disaster recovery plans. [15.]

The drawbacks of cloud computing are limited access to and control of infrastructure and security issues. In addition, a reasonably fast internet connection and high bandwidth are required. [15.]

3 Amazon Web Service

3.1 About Amazon Web Services

Amazon web services is a platform that provides cloud computing services. Amazon web services was launched in 2006. The idea of introducing Infrastructure as a service started in 2003. It is providing cloud services to customers in the form of web services. Currently, Amazon web services provides services throughout the world in a number of countries. The Amazon services are low cost, scalable and reliable. Businesses are boosted by acquiring the benefit of cloud services. The data centers of Amazon are located in different parts of the world to provide efficient services to customers. The platforms of Amazon web services deliver solutions to customers. Some of the solutions are backup and storage, content delivery, websites, application hosting, databases, and enterprise information system technologies. [19.]

Amazon is one of the giant cloud services providers. According to Canalys, which is a leading global technology market analyst firm, AWS has had the market share of 32.4 % as of February 2020. Microsoft Azure, Google cloud, Alibaba cloud, and other clouds have a market share of 17.6%, 6%, 5.4%, and 38% respectively. [20,35.]

3.2 Shared Responsibility Model

Security and compliance are a shared responsibility that clearly define accountability of customers and AWS. The customer responsibility depends on their choice of cloud services from AWS. This model benefits the customer by avoiding configuration and administration at physical layers, virtualization and the operating system. In this model, the customers are responsible for installation, configuration and management of applications, the operating system and group security based on rules and regulations of IT services. [33.]

AWS manages and administers global infrastructure such as storage, computing, databases, networking, software and hardware. There are controls managed by either AWS or customers, or both. The customer inherits the controls of the environment and physical

infrastructure. In shared controls, AWS is responsible for the infrastructure and customers have the freedom of implementing controls that meet their requirements. In general, AWS manages the security of the cloud, the and customer manages the security inside the cloud. [33.]

Figure 2 shows the shared responsibilities between AWS and the customer.

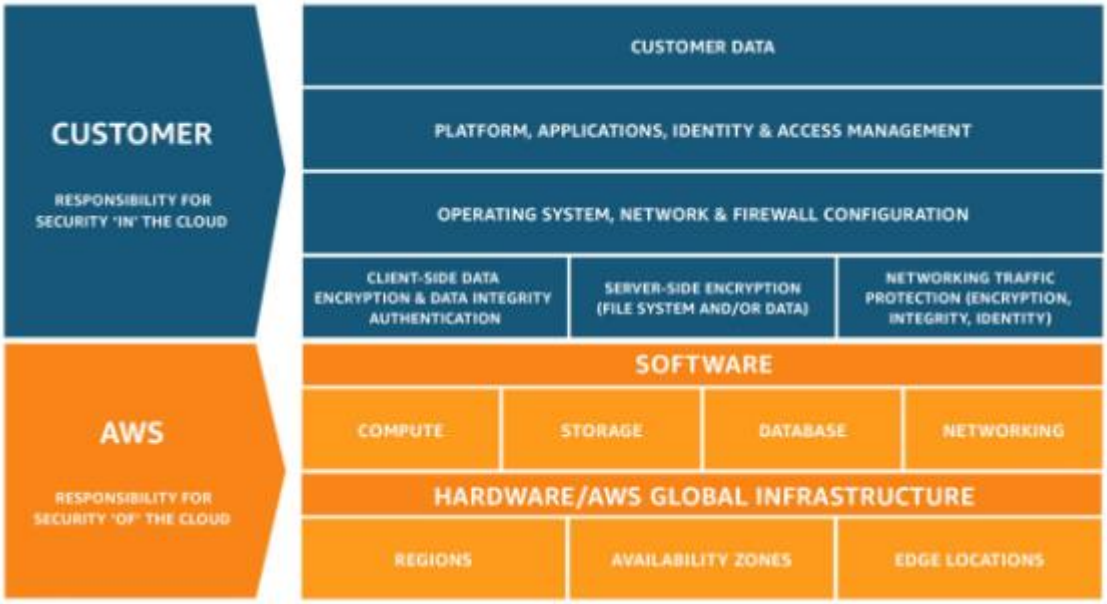


Figure 2. Shared responsibility model, Copied from Amazon Web Services [33]

3.3 Regions and Availability Zones

AWS sets up and organizes clusters of data centers throughout the world. The place where the cluster is located is called Region. The data centers in a region together form Availability zones. Currently, the cloud infrastructure of AWS consists of 23 regions and 73 availability zones that provide services to 245 countries. [35; 36.]

Every region of AWS is independent of each other. Each region consists of a number of availability zones. The availability zones in a region are physically isolated. The regions are formed with a high standard of safety and security. [35; 36.]

Availability zones are made of several data centers. Each data center is occupied with fault tolerant connectivity, network, and power supply. The interconnection between availability zones has low-latency and higher bandwidth. The availability zones are located in a reasonable distance to each other. [35; 36.]

3.4 Solutions Provided by Amazon

AWS is one of the cloud computing service providers in the market. The services, applications and solutions from AWS are increasing continuously. Amazon provides a range of services to customers. Some of the services include storage, databases and computing. [20.]

Storage and Backup

One of the solutions of the Amazon web services is storage and backup. For instance, Amazon S3 is a cutting-edge object-based storage technology that gives the best performance, scalability and availability of data. Customers of S3 can store, retrieve and secure their data. The type of data that can be hosted on S3 comes from different sources such as applications of enterprises, mobile applications, websites, data analytics, and IOT endpoints. The management and controlling features of Amazon S3 are easy and user friendly to use, access and configure. Data can be manipulated to fulfill the specifications required by organizations and business processes. [21.]

Amazon S3 benefits users by saving cost without affecting performance. It also secures data so it cannot be accessed by unauthorized users using encryption tools. Data can be accessed whenever needed, and it is protected from threats. Access permission can be granted with limitations. Querying and analyzing data using tools such as Amazon Athena and Amazon Redshift spectrum is possible. Finally, Amazon S3 has a network of partners to support storage service on the cloud. [21.]

Furthermore, AWS provides more storage services such as Glacier, Elastic Block Store (EBS), Elastic File System (EFS), Storage Gateway and Snowball. For instance, Glacier

is a good option for archiving of data, and EBS is block storage with low latency and high availability.

Content Delivery

Amazon CloudFront was designed for delivery of content. It delivers applications, data, and videos. The delivery system of CloudFront is achieved through fast speed transferring, minimized latency and a friendly interface. CloudFront is integrated with EC2, Elastic Load Balancing (ELB) and Amazon S3 to boost users' access. The CloudFront security offers reliable protection on application and network layers. It can be programmed to apply for particular applications, and it can be integrated with a number of services for speedy, worldwide services. [22.]

Enterprise IT

AWS is the most preferable cloud service provider to accelerate business with minimized risks. The set of functionalities and innovations with a secured cloud makes AWS the choice of companies. The cloud service always goes in parallel with the customers' demand and business environment and comes up with the right solutions to achieve higher revenue by increasing productivity and minimizing risks. [23.]

Application Hosting

Before the birth of the cloud, companies used to invest on infrastructure to run their business applications. The software as a service (SaaS) model of cloud computing avoids the huge investment and time to host and run applications. It is good to make assessment to find out the specific requirements to host applications on the cloud. The requirements could include finding out what the right platform is to run applications if the existing on-premises operating systems are used and what are the service of the cloud provider is with respect to commitments, response time to inquiry, and security. [24.]

Databases

The Amazon database service has an option of 15 database types for customers. The database type includes time series, in-memory, key-value, a ledger and a graph. The various available database can provide solutions to a set of problems or a specific problem. A database running on the AWS cloud platform is fully managed when it comes to configuration, setup, backup and restoring (?). The latency of the database is in microsecond without downtime. [25.]

AWS database services can be grouped based on database type. SQL is a relational database system that models data in the form of a table. A relational database has properties of ACID (atomicity, consistency, isolation, and durability). A relational database is good for online transaction. On the other hand, the NoSQL database is flexible and fast which is suitable for processing a huge amount of data with low latency. AWS allows databases to be created in the form of SQL or NoSQL. SQL (Amazon Aurora, Amazon RDS, Amazon Redshift) and NoSQL (DynamoDB, Neptune, QLDB) are good examples. [25.]

Web Hosting

Web hosting is a service from AWS which gives hosting to applications and websites. The web hosting solutions provide different options to give the right solutions to customers that are hosted on AWS. The Amazon web service supports several content management systems and platforms such as Joomla, WordPress, Drupal, Node.js, Java, and Rub. Data centers are available everywhere in the world so that customers can host their website any location of their choice. The infrastructure can scale up or down according to the website traffic that varies throughout the day. The website solution from AWS can be applied to host simple websites, web applications, static websites, and enterprise web hosting [26.]

Table 1 below shows the classification of Amazon Web Services.

Table 1. Classification of Amazon web services

Compute	Storage	Applications	Network	Security & identity
• Elastic cloud compute (EC2) • EC2 container registry • Amazon light sail • ELB • VPC • Beanstalk • Lambda	• Elastic File System • S3 • Glacier • Storage gate-way • Snowball	• Work Docs • Workspaces • Work Mail • Amazon	• Route 53 • CloudFront • VPC • ELB	• Artifact • Inspector • Directory Service • IAM • KMS • WAF

3.5 Benefits of Amazon Web Services

Amazon Web services (AWS) is a cutting-edge technology for all types of businesses that demand low cost, scalable and reliable services from cloud computing. The geographical span of AWS extends to 22 regions with number of services of data storage, development of applications and games, business analytics, and more services. [27.]

The benefit of AWS can be measured with different parameters of security, flexibility, scalability, reliability, ease of use, and cost. The AWS infrastructure is well secured at every layer of communication. The user-friendly environment of AWS facilitates an application hosting in a secured manner. Scaling computing resources up and down according to the demand of an application can be achieved using the AWS tools, such as Elastic Load Balancing (ELB) and Auto Scaling. The AWS environment supports most operating systems, databases, web platforms and programming languages so that the user can choose the required technologies freely and smoothly. Furthermore, the AWS infrastructure is reliable and cost effective.

4 Implementation

For the purpose of the implementation, a case study was carried out in a financial service institution.

4.1 Traditional IT system of financial service institution

In a traditional IT system of the financial service sector, infrastructures are hosted and managed on premises. The local network system encompasses only resources in the head office. Branch offices usually many not have connected with a wide area network to share resources with the head office. Information sharing between the offices has been done through email and post.

On-premises IT infrastructure may consist of the following:

- The core banking system that may run on Linux or Windows server with relational or non-relational database backend.
- Windows Active directory server to store and manage information about objects in the network.
- ISA (Internet Security and Acceleration Server) for controlling internet usage based on predefined policies and procedures.
- The website of the company being hosted at the local hosting company.

Figure 3 below shows a typical on-premises IT infrastructure of a financial institution.

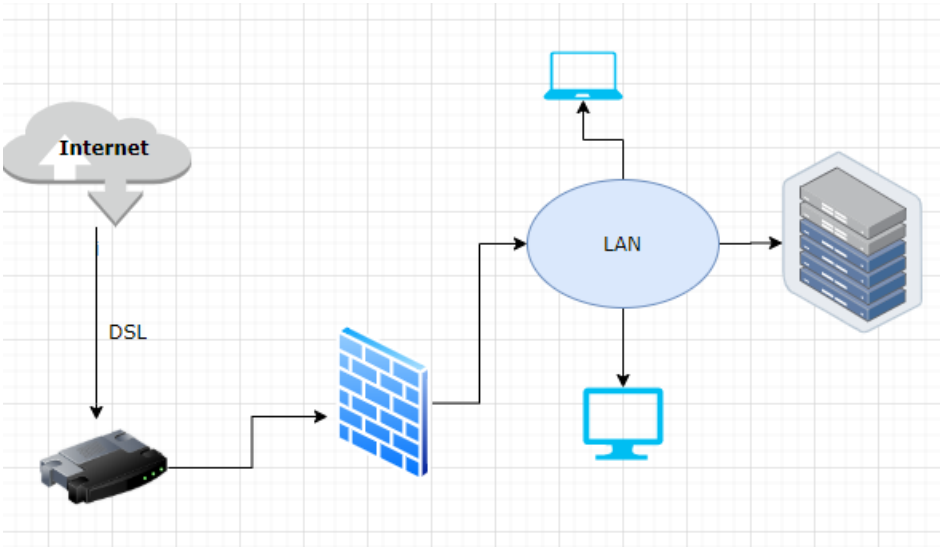


Figure 3. The existing on-premises IT infrastructure

A shown in Figure 3, a traditional IT infrastructure for a financial service institution host and administration runs locally.

The existing on-premises IT infrastructure is unable to address the following issues:

- optimal performance and reliability
- accommodating the continuous change and growth in the system
- high capital investment of upgrading the system
- time consuming process of purchasing and deployment of hardware and software

4.2 Infrastructure Architecture with AWS

The infrastructure is designed to confirm the best practices of AWS. It has integrated VPN connection to securely connect the remote office. The data stored at AWS is secured by encrypting data using AWS Key Management services (KMS). AWS CloudTrail is implemented for audit logging.

Users, Groups and Roles

The system administrator has an administrative privilege on resources. Database administrators have full access to Amazon RDS, and members of monitoring groups have limited access, i.e. read-only access, to EC2 and S3.

In addition to using a username and a password, it is a good practice to use Multi-Factor Authentication (MFA) for extra security.

Table 2 below shows the role of each group and their access permission.

Table 2. Users, groups and roles

Users, Groups and Roles		
Group/Role	**Group/Role Name**	**Permissions**
Group	sysadmin	Administrator Access
Group	dbadmin	AmazonRDSFullAccess
Group	monitoring	AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess, AmazonRDSReadOnlyAccess
Role	EC2toS3	S3: Get*, S3: List*, S3: Put*

VPC (Virtual Private cloud) is a virtual network in a separate part of the AWS cloud that is managed systematically to create AWS resources. The owner of the VPC has full access to create Subnets, IP addresses, network gateways and routing tables. [16.]

Table 3. Details of the virtual private cloud.

VPC design			
VPC	Subnets	Availability Zone	CIDR range
1	8	2	10.0.0.0/16

The subnet represents a set of IP addresses inside the VPC. The subnet design table contains the name of the subnet, availability zone, subnet type, and address for each subnet.

Table 3. Details of Subnets

Subnet Design			
Name of Subnet	Availability Zone	Type of Subnet	Subnet address
Public1	a	Public	10.0.10.0/27
Public2	b	Public	10.0.20.0/27
WebPrivate1	a	Private	10.0.30.0/24
WebPrivate2	b	Private	10.0.31.0/24
AppPrivate1	a	Private	10.0.40.0/24
AppPrivate2	b	Private	10.0.41.0/24
DBPrivate1	a	Private	10.0.50.0/24

DBPrivate2	b	Private	10.0.51.0/24

An instance is defined as a virtual server located inside the cloud. The type of the instance defines the hardware to be used. An instance type provides varieties of memory and computing features. Once an instance is launched, it is like a normal computer that can be used and managed. [17.]

Two instances were deployed on the Web and Application tier as the minimum number of instances, and the number of instances increased according to the defined conditions.

Table 5 describes the instance type and the operating system in each tier.

Table 5. Details of instances

Tier	Operating System	Type	No. of Instances
Web	Windows Server 2016 Base	t3.large	2
App	Linux	c4.xlarge	2
DB	Oracle	d2.xlarge	N/a

Elastic Load Balancing is a tool used to transmit data and applications to numerous destinations. The destination could be Availability zones, Instances, IP network or containers. Load Balancer manages traffic by sharing the load among available instances. Load Balancer controls the health and takes care of decryption and encryption of resources.

Table 6. Details of Load Balancers

Load balancer	Name	Type	Subnets	Source
Web tier	dbe-web-elb	external	Public01/Public02	All
App Tier	dbe-app-elb	internal	AppPrivate01/AppPrivate02	web-tier

The table below shows the security group for each tier with a specific rule. Port 80 is opened for the web and application tier and port 1433 is opened for the database tier.

Table 7. Details of Security Group (SG)

Instance Tier	**SG Name**	**Rule**
Web tier	DBE-web-sg	Allow port 80
App Tier	DBE-app-sg	Allow port 80
Database tier	DBE-db-sg	Allow 1433

Auto scaling is one of the applications provided by AWS that allows scaling and configuring resources spontaneously. Numerous AWS services are organized and accessible at a single point in a user-friendly interface to scale and configure resources. Table 7 below shows the auto scaling configuration for web and application tier. [18.]

The table 7 below shows Autoscaling configuration design on web and app tiers.

Table 7. Details of Auto Scaling configuration

Tier	**OS**	**Type**	**Security Group**
Web	Windows Server 2016 Base	t3.large	DBE-web-sg
App	Linux	c4.xlarge	DBE-app-sg

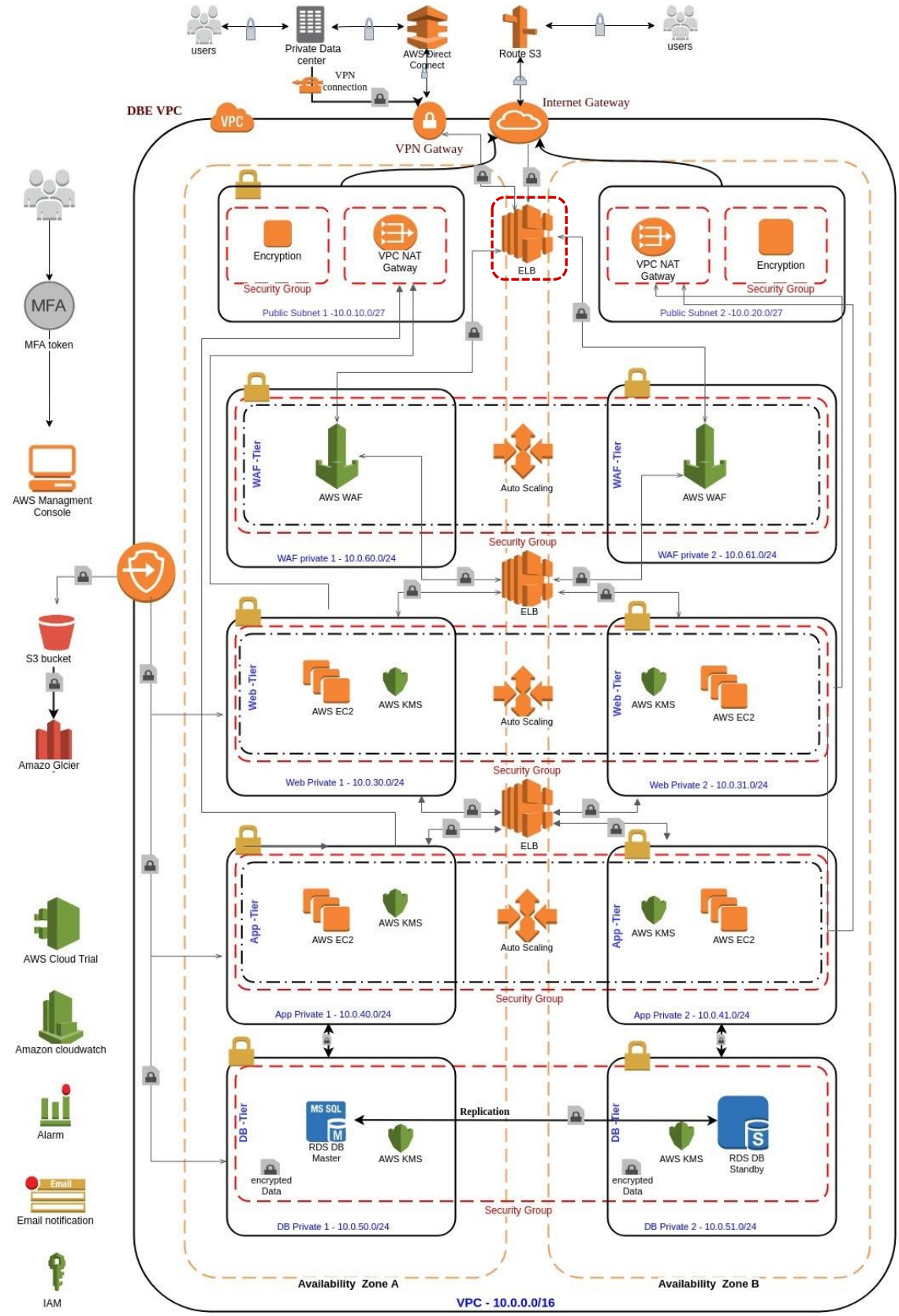


Figure 4. Architecture diagram

As shown in figure 5, the architecture diagram contains three tiers (Web, Application and Database). Each tier is bounded by a security group to control traffic going in and out of the resources. In addition, the AWS WAF tier implemented to safeguard web applications from attacks.

Elastic Load Balancing is one of the networks and content delivery components that is implemented for the purpose of distributing traffic and finding out failed instances to achieve high availability. The public ELB is protected with a security group and configured to allow appropriate traffic. WAF protects the web services and applications based on defined rules and conditions. Furthermore, the architecture increases or decreases instances based on the load of the application using Auto Scaling. Two instances are deployed on the Web and App tier as the minimum number of instances and the number of instances increased according to the defined conditions to maximum of four instances.

In addition, the architecture diagram shown in Figure 4 contains the following components.

- AWS Direct Connect to have high speed direct connection between the institution data center and AWS.
- VPN connection to connect VPC to an on-premises network securely.
- NAT gateways to connect instances in the web and app tiers to the internet.
- Route 53 to route users' requests to resources in AWS.
- S3 bucket and Amazon Glacier for storage services.
- AWS CloudTrail to monitor account activities.
- Amazon CloudWatch for resource monitoring.
- IAM for management of user access to resources.

4.3 Implementation on AWS Cloud

A free tier AWS account is created to have free access to AWS services and platforms for hands-on practical implementation. This thesis has discussed only the main and key parts of the implementation such as IAM, storage, database, computing and networking services.

AWS accounts are created for management of services and accounts. Three groups are created based on the best practices of AWS for access permission. The group names are dbadmin, monitor and sysadmin. Under each group, two users were created. Each group has granted the following access permissions.

- Sysadmin - administrator access
- Dbadmin - Amazon RDS full access
- Monitor - ReadOnlyAccess on EC2, S3 and RDS.

Data are protected while in transit or at rest. Encryption at rest is applied on user data, such as usernames, passwords and email. Secure Sockets Layer (SSL) secures all data in transit. All keys are managed by the AWS key management.

To meet the business requirements, the security configuration should be audited. The proper access permission of users, groups, roles and policies was achieved through auditing in an interval of time. AWS CloudWatch was integrated for monitoring.

S3 bucket and Amazon Glacier were implemented for backing up and long-term archiving of data respectively. Traffic flow in and out of the VPC to the S3 bucket and Amazon Glacier through endpoint.

Account creation

A free account shown in Figure 5 below was created for the purpose of implementing and testing the architecture design.

The AWS free tier offers a free service to explore numerous products for a period of 12 months. The offer includes 750 hours of free access on Amazon EC2; 5GB object storage on Amazon S3; 750 hours of access to Amazon RDS for SQL server, MariaDB, MySQL, and PostgreSQL; and 25 GB of NoSQL database of Amazon DynamoDB. For the deployment of the machine learning platform, AWS offer 250 hours of access to Amazon SageMaker. In addition, it offers millions of AWS Lambada run codes based on events, 750 hours of Amazon LightSail for 30-days free trial and 30 days Amazon Guard Duty for monitoring and identifying threat. [29.]

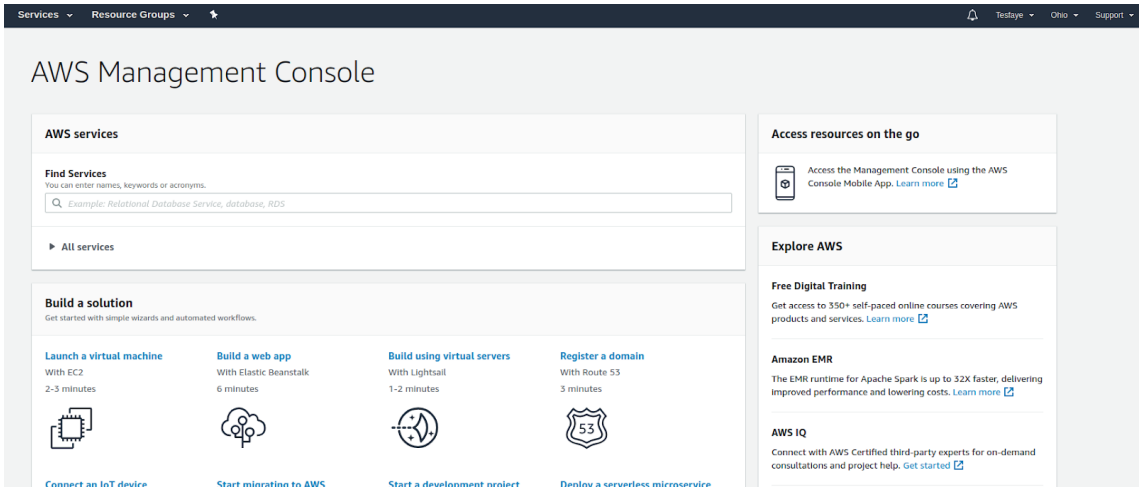


Figure 5. AWS account

User, Groups and Roles

A user can represent a person or software, for example a Python client. Users have a specific identity in a security group. For a better management of users, it is good to include users in a group. Each group has their own specific privileges on the level of system administration, monitoring and database access. [30.]

Figure 6. Users, Groups and Roles

Creating a Virtual Private Network (VPC)

Implementing Virtual Private Network (VPC) offers the following benefits:

- VPC controls traffic that is coming into and going out of subnets and instances.

- The AWS Management console is a user-friendly environment to create VPC, and to configure the appropriate range of IP addresses, routing tables, and subnets. These features help to minimize the time spent configuring and setting up network infrastructure.

- It is customizable which enables creating, configuring and administering the address/addresses, network gateways, and routing tables of the subnet freely. [16.]

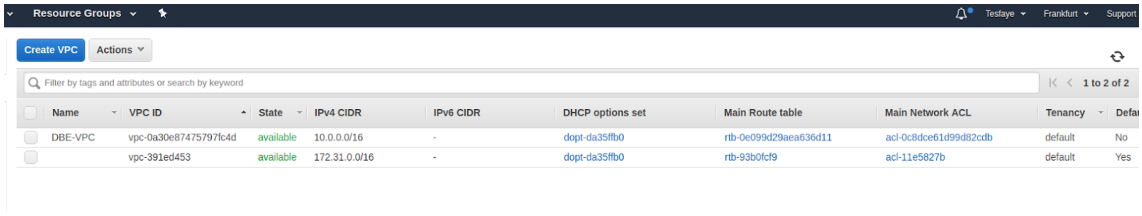


Figure 7. Virtual Private Network (VPC)

Figure 8 below shows the subnets created in the availability zones. Each subnet has assigned IPv4 address.

Creating Subnets

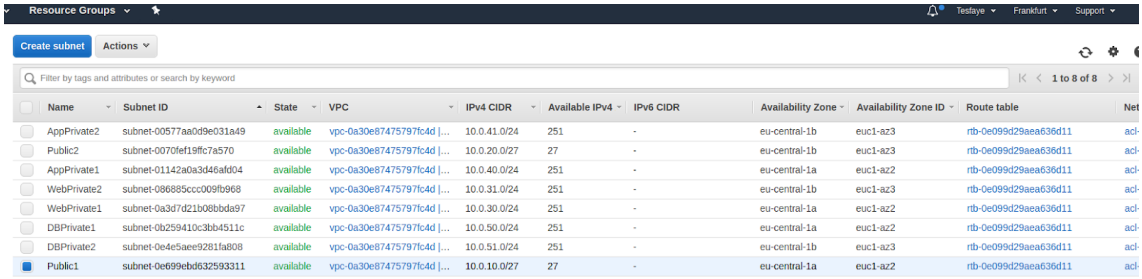


Figure 8. Subnets

Internet Gateway

An internet gateway is part of a VPC which facilitates communication between the internet and a private VPC. Basically, the Internet gateway provides services of Network Address Translation (NAT), directing traffic to the VPC that is routed to the internet.

The following steps should be done to a VPC to activate access to the internet:

- Creating a link / links between VPC and internet gateway
- Creating routing a table / tables to private and public subnets
- Assigning an IP address / addresses to instances in the subnet

- Setting up a security group / groups and an access control list / access control lists in order to control the routing in and out of the instance. [31.]

Figure 9 below shows the internet cofiguration design

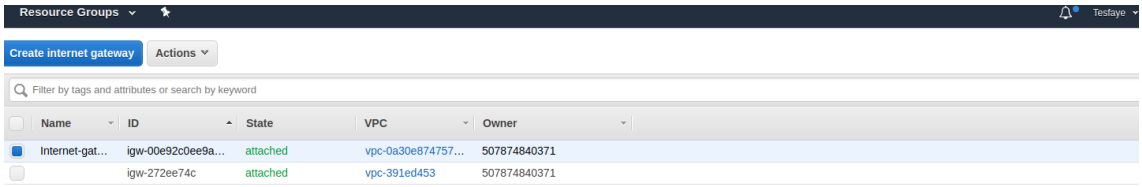


Figure 9. Internet gateway

Figure 10 below shows the routing of traffic in and out of the VPC. Two subnets are associated to external routing and six subnets to internal routing.

Route table

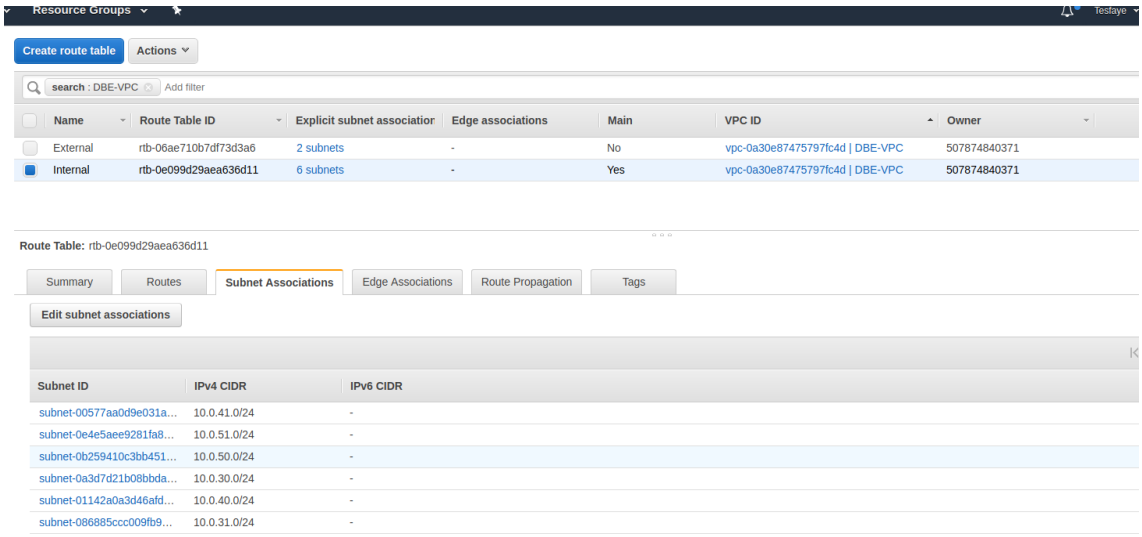


Figure 10. Route table

Security Group

The security group is a firewall for an instance that manages egress and ingress traffic. The security group is applied on instances. Security groups can be assigned for every instance in a subnet.

Inbound and outbound traffic of a security group should meet the following regulations:

- The source of the traffic can come from a single IP address, a range of IP addresses or another security group.
- The traffic destination could be an IP address or number of IP addresses in a different security group.
- It is possible to define ICMP.

- It is recommendable to specify description to a security group. [31.]

Figure 11 below shows security group created for each resource.

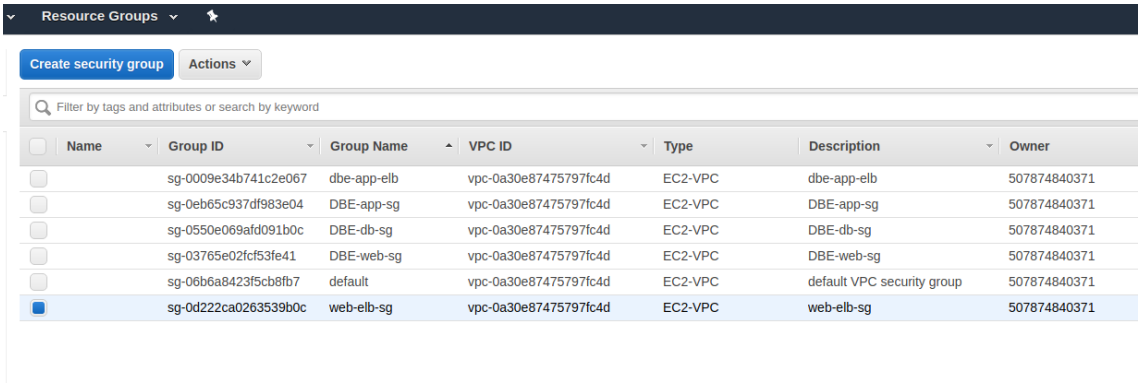


Figure 11. Security group

Instances

An instance is defined by an AMI that sets up the type of the operating system and applications. Every instance comes up with a variety of memory and hardware. An instance is like a normal computer that can be interacted with. [17.]

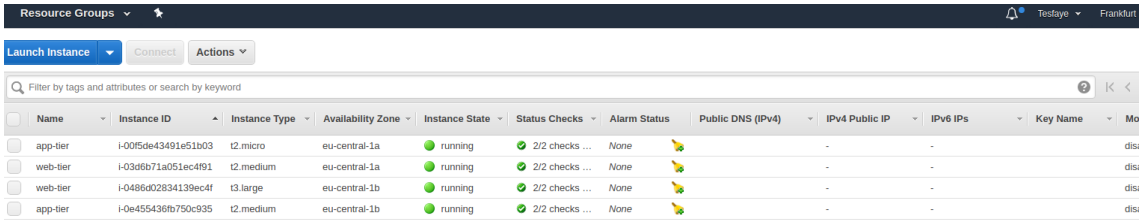


Figure 12. Instances

Database

AWS provides a variety of database types that are suitable for different purposes. AWS services offer database services that suit an application. The following list offers examples of these services (?):

- Amazon DynamoDB for e-commerce, web applications with huge traffic.
- Amazon RDS for an application of customer relation management and enterprise resource planning.
- Amazon Document DB for a content management system / content management system.
- Amazon Timestream for an application of the Internet of Things. [26.]

Figure 13 below shows the database created inside the VPC. Oracle standard edition is applied as engine for the database.

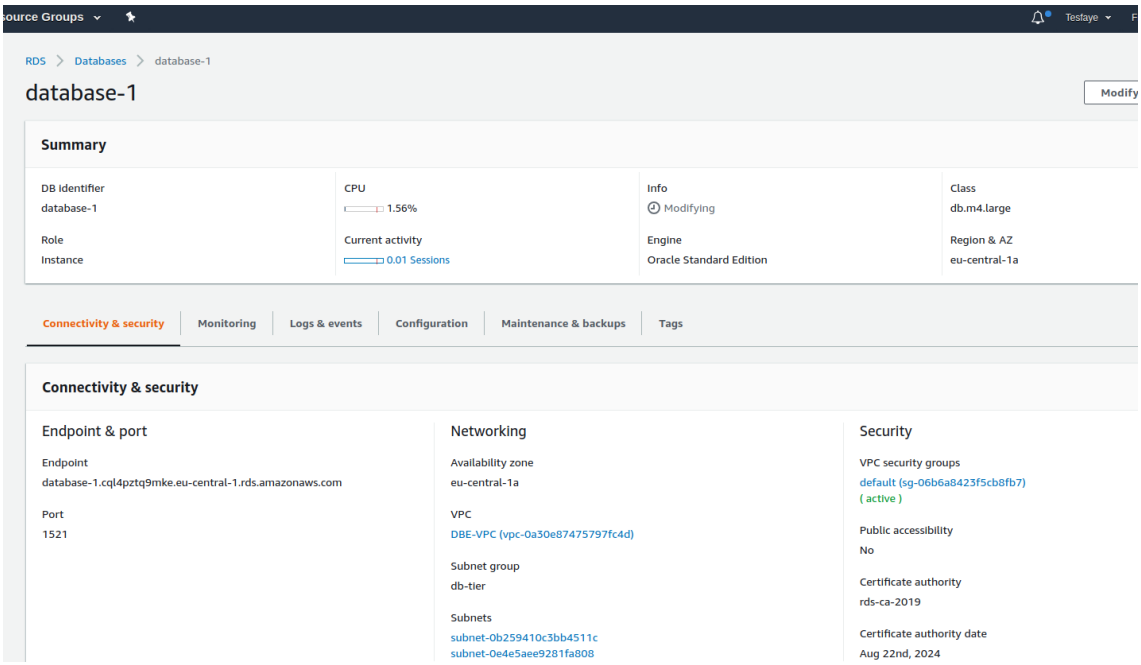


Figure 13. Databases

Load Balance

Elastic Load Balancing (ELB) balances traffic by distributing it to the required destination. Elastic Load Balancing manages the traffic by scaling it up and down based on the load of the application.

Elastic Load Balancer can offer the following benefits:

- Balancing traffic load of instances¨
- Increasing and decreasing the number of the instances
- Controlling the health situation of instances. [34.]

Figure 14 below shows load balance design on application and web tiers.

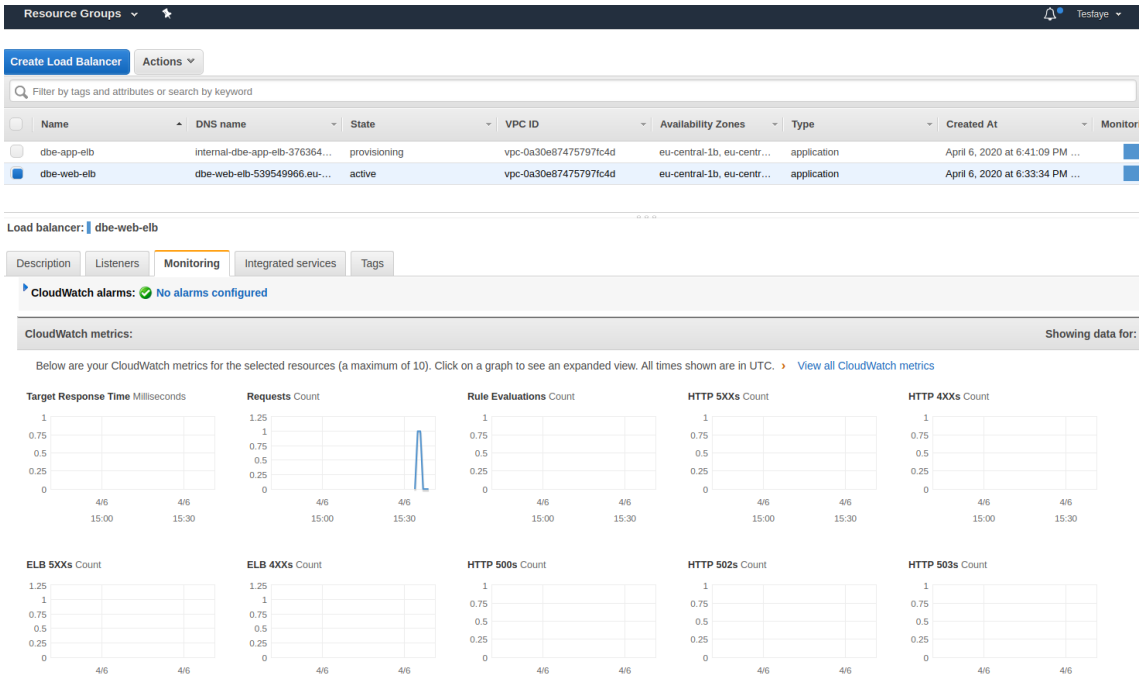


Figure 14. Load balance

Auto Scaling

Auto Scaling is a feature used to scale up and down resources for an application that face change in traffic. Auto scaling manages scaling resources such as EC2 to start and stop. As a minimum requirement, two instances are running on each Application and Web tier. The instance would increase to a maximum of four based on the load of the application.

Normally Auto scaling takes action based on metrics. The forecast of the scaling depends on traffic analysis in a time interval of two weeks. Based on the traffic it increases or decreases resources. [18.]

Figure 15 below shows the two-auto scaling group created. The auto scaling group created on web and applications tier.

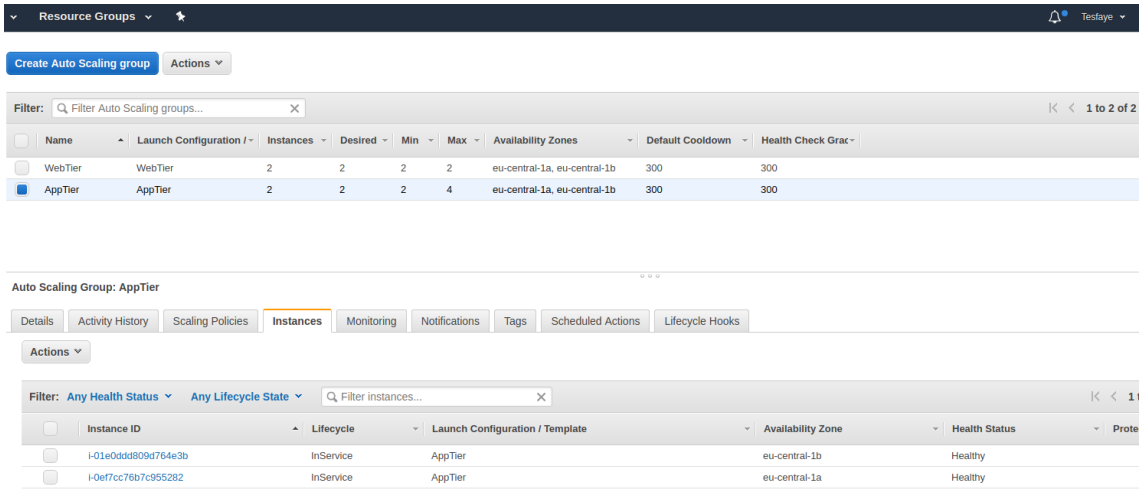


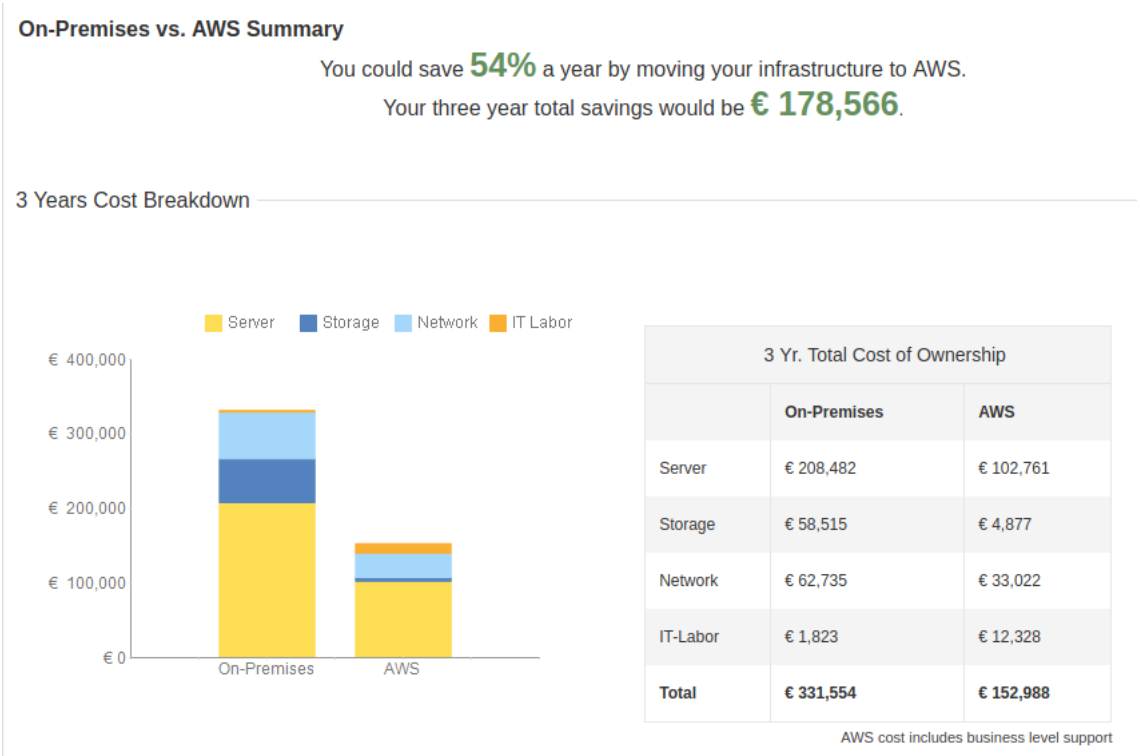
Figure 15. Auto Scaling

5 Results and Discussion

Migration of the on-premises information system of the financial service institution to the cloud using Amazon Web Services benefits the company in different ways. Amazon Web Services enables the company to utilize the services of storage, networking, infrastructure, database and security efficiently. The network infrastructure services managed to connect all the branch offices and users globally from anywhere. The branch offices have equal access to the core system of the financial services institution. For instance, tools and technologies from the AWS services create a platform to analyze and query data for better decision making and improve customer services and satisfaction.

One of the benefits of transforming an on-premises IT system to the cloud is cost minimization on server, storage, networking, data transfer, and IT labor costs. Based on the proposed design, as shown in Figure 16 the financial institution could save 54% a year and 178,566 euros in total in three years.

Figure 16 below shows the cost of on-premises vs AWS, which was calculated based on AWS Total Cost of Ownership (TOC) calculator (awstcocalculator.com).



3 Yr. Total Cost of Ownership

	On-Premises	AWS
Server	€ 208,482	€ 102,761
Storage	€ 58,515	€ 4,877
Network	€ 62,735	€ 33,022
IT-Labor	€ 1,823	€ 12,328
Total	**€ 331,554**	**€ 152,988**

AWS cost includes business level support

Figure 16. AWS Total Cost of Ownership (TOC) calculator

The migration to the AWS cloud systems provided the following benefits to the financial institution:

- Reduction of expenses of capital, support and administrative costs.
- Achieving the demands of the bank in terms of security, reliability and performance.
- Acquiring cloud based modern information technology assets and infrastructure to boost customer satisfaction.
- Moving the core system of the financial service institution to the cloud for the branch offices to have equal access to resources with the head office and provide full services.
- Enabling taking advantage of the cloud services to use tools and technologies for data and business analysis.

The application and scope of the Amazon Web Service is broad, and it encompasses infrastructure, artificial intelligence, machine learning, the Internet of Things and analytics. However, this project is limited to infrastructure design, implementation and application.

The aim of this project was to migrate the traditional information system of the bank to cloud computing using the Amazon Web Services technology. For the purpose of the implementation, a 3-tier architecture was designed with one public and two private subnets. The private subnets host the Application tier and the Database tier.

The Web and Application tier run Amazon EC2 instances that were installed and configured with the appropriate operating system and configuration. A security group was created, and each Amazon instance was placed in the security group with defined inbound and outbound traffic rules. Communication of the instances between the virtual private cloud and the internet routed through the Internet gateway. Furthermore, Elastic Load Balancing (ELB) was included in the architecture for the distribution of application traffic,

to identify unhealthy instances and to provide a solution. Finally, Auto scaling was implemented so that the architecture can respond to changes in demand for resource utilization.

In addition, monitoring the instance in the virtual private cloud was done using Amazon CloudWatch. Amazon CloudWatch operates in the real-time fashion to collect and analyze data, notify for action to be applied according to the specified metrics.

6 Conclusion

The goal of the study was to migrate the traditional IT system of a bank to the cloud using the Amazon Web Services (AWS) technologies. The implemented 3-tier architecture design migrated the on-premises infrastructure to the cloud to ensure business continuity.

In general, the process of the transformation involved three basic steps. First, studying and analyzing the requirement of the infrastructure was needed. Second, designing 3-tier architecture on web tier, application tier and database tier was done. Finally, the design was implemented using the AWS technologies. Different AWS services such as EC2, ELB, auto scaling and databases were used. The implemented cloud computing system resulted in boosting productivity and flexibility by cutting down IT costs.

According to the AWS Total Cost of Ownership (TOC) calculator, the financial institution could save 54% of its expenses on server, storage, network, and IT labor if all calculations are taken into account. The proposed design would cut down 178,566 euros of costs in three years.

Even if cloud computing encompasses a broad range of technologies, only some technological aspects were studied in this thesis. The major issues in cloud computing are security, privacy, compliance and sustainability, and they need further studying.

References

1. Rountree, D., Castrillo, I. & Jiang, H. The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice. Electronic book. Syngress; 2013.

2. Wang L, Ranjan R, Chen J, Benatallah B, editors. Cloud Computing: Methodology, Systems, and Applications. Electronic book. Baton Rouge: CRC Press LLC; 2011.

3. Peter Mell (NIST), Tim Grance (NIST). The NIST Definition of Cloud Computing [online]. September 2011.
URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed April 22, 2020)

4. Murugesan S, Bojanova I, editors. Encyclopedia of Cloud Computing. Electronic book. New York: John Wiley & Sons, Incorporated; 2016.

5. Schouten, E. Cloud Computing Defined: Characteristics & Service Levels [online]. January 31, 2014. URL: https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/ (accessed January 7, 2020)

6. AnkitMahali. Characteristics of Cloud Computing [online].
URL:https://www.geeksforgeeks.org/characteristics-of-cloud-computing/ (accessed January 8, 2020)

7. Microsoft. Cloud Deployment Models [online]. 2020.
URL: https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/4-cloud-deployment-models (accessed January 9, 2020)

8. Open Group. Cloud Computing for Business – What is cloud? [online]. 2016.
URL:http://www.opengroup.org/cloud/cloud_for_business/p1.htm (accessed January 9, 2020)

9. Microsoft. What Are Public, Private, and Hybrid Clouds? [online]. 2020.
URL: https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/ (accessed January 9, 2020)

10. IBM Cloud Education. Hybrid Cloud [online].16 October 2019.
URL: https://www.ibm.com/cloud/learn/hybrid-cloud (accessed January 24, 2020)

11. Open Group. Cloud Computing for Business – What is Cloud? [online]. 2016
URL: http://www.opengroup.org/cloud/cloud_for_business/p1.htm#X_Service_Models (accessed January 27, 2020)

12. ICT Solutions for Brilliant Minds. Concept of Cloud Computing [online].
URL: https://docs.csc.fi/cloud/concepts/ (accessed January 27, 2020)

13. IBM Cloud Education. IaaS (Infrastructure-as-a-Service) [online]. July 12, 2019.
URL: https://www.ibm.com/cloud/learn/iaas (accessed January 27, 2020)

14. IBM Cloud Education. PaaS (Platform-as-a-Service) [online]. October 29, 2019. URL: https://www.ibm.com/cloud/learn/paas (accessed February 06, 2020)

15. Microsoft. Benefits of Cloud Computing [online]. 2020. URL:https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/3-benefits-of-cloud-computing (accessed February 11, 2020)

16. Amazon Web Services. Amazon Virtual Private Cloud [online]. 2020. URL:https://aws.amazon.com/vpc/ (accessed February 25, 2020)

17. Amazon Web Services. Instances and AMIs [online]. 2020. URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instances-and-amis.html (accessed February 25, 2020)

18. Amazon Web Services. What is AWS Auto Scaling [online]. 2020. URL: https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html (accessed March 5, 2020)

19. Amazon Web Services. About AWS [online]. 2020. URL: https://aws.amazon.com/about-aws/ (accessed April 7, 2020)

20. Scott Carey. The History of AWS: A Timeline of Defining Moments from 2002 to now [online]. March 12, 2019. URL:https://www.computerworld.com/article/3412382/the-history-of-aws--a-timeline-of-defining-moments-from-2002-to-now.html#slide2 (accessed April 7, 2020)

21. Amazon Web Services. Amazon S3 [online]. 2020. URL: https://aws.amazon.com/s3/ (accessed April 10, 2020)

22. Amazon Web Services. Amazon CloudFront [online]. 2020. URL: https://aws.amazon.com/cloudfront/ (accessed April 10, 2020)

23. Amazon Web Services. AWS in the Enterprise [online]. 2020. URL: https://aws.amazon.com/enterprise/ (accessed April 10, 2020)

24. Amazon Web Services. Application Hosting [online]. 2020. URL: https://aws.amazon.com/application-hosting/ (accessed April 10, 2020)

25. Amazon Web Services. Database on AWS, The Broadest Selection of Purpose-Built Databases for All Your Application Needs [online]. 2020. URL: https://aws.amazon.com/products/databases/ (accessed April 10, 2020)

26. Amazon Web Services, Web Hosting [online]. 2020. URL: https://aws.amazon.com/websites/ (accessed April 10, 2020)

27. Rajnish Kumar Sharma. What Is Amazon Web Services and Why Should You Consider it? [online]. January 23, 2020. URL: https://www.netsolutions.com/insights/what-is-amazon-cloud-its-advantages-and-why-should-you-consider-it/ (accessed April 11, 2020)

28. Amazon Web Services. Benefits at a Glance [online]. 2020. URL: https://aws.amazon.com/application-hosting/benefits/ (accessed April 11, 2020)

29. Amazon Web Services. AWS Free Tier [online]. 2020. URL: https://aws.amazon.com/free/?all-free-tier.sort-by=item.additional-Fields.SortRank&all-free-tier.sort-order=asc (accessed April 12, 2020)

30. Oracle. Users, Groups, and Security Roles [online]. 2020. URL: https://docs.oracle.com/cd/E11035_01/wls100/secwlres/secroles.htm (accessed April 12, 2020)

31. Amazon Web Services. Internet Gateways [online]. 2020. URL: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html (accessed April 12, 2020)

32. Amazon Web Services. Security Groups for Your VPC [online]. 2020. URL:https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html (accessed April 14, 2020)

33. Amazon Web Services. Shared Model [online]. 2020. URL: https://aws.amazon.com/compliance/shared-responsibility-model/ (accessed April 14, 2020)

34. Amazon Web Services. What Is Elastic Load Balancing [online]. 2020. URL: https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html (accessed April 14, 2020)

35. Amazon Web Services. Regions and Availability Zones [online]. 2020. URL: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (accessed April 24, 2020)

36. Amazon Web Services. Regions and Availability Zones and Local Zones [online]. 2020. URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-availability-zones (accessed April 24, 2020)

37. Katy Stalcup. AWS vs Azure vs Google Cloud Market share 2020: what the latest Data Shows [online]. February 5,2020. URL: https://www.parkmycloud.com/blog/aws-vs-azure-vs-google-cloud-market-share/?fbclid=IwAR0BilpLhRH350baW4_pS4SkZr7AHnoqAl5CUhjopqiVdRR9BuJvZcfsu00 (accessed April. 29, 2020)